PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-238306
(43)Date of publication of application : 31.08.1999

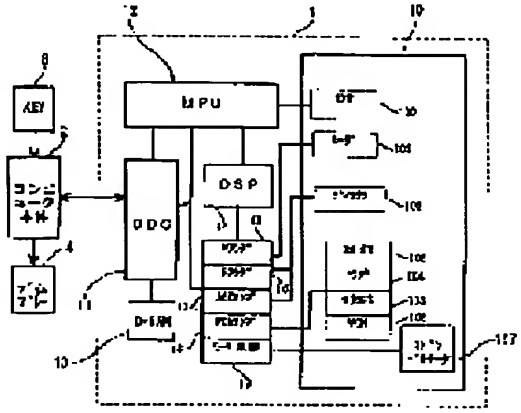
(51)Int.Cl. G11B 20/10
G11B 19/04
// G11B 7/00

(21)Application number : 10-038840
(22)Date of filing : 20.02.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : IMAMURA KIYOMI
YAMAKAWA TERUJI

(54) INFORMATION STORAGE DEVICE AND CONTROL METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the secrecy of recorded data of a storage medium by making an information storage device impossible to get access to data of an inserted storage medium when the intrinsic identification sign of the information storage device which is previously recorded in the prescribed area of the storage medium and the identification sign of the storage device into which the storage medium is inserted do not coincide.
SOLUTION: Relating to a data storage device 1, an MPU 12 controls the whole of the device and a magneto-optical disk control part (ODC) 11 reads out the identification sign of the medium management information of an inserted magneto-optical disk to perform a security processing. When the identification signal is in an initial state, the OCD 11 permits the reading/writing of data and when data are written on the disk, the ODC 11 judges whether the sign of the disk coincides with that of the data storage device 1 or not. As a result, when they coincide, the ODC 11 permits the reading/writing of data, however, when they do not coincide, it inhibits the reading/writing of data. Thus, even when the inserted magneto-optical disk is plagiarized, the secrecy of the data is secured.



LEGAL STATUS

[Date of request for examination] 28.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－238306

(43)公開日　平成11年(1999)８月31日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
19/04	５０１	19/04	５０１Ｈ
// Ｇ１１Ｂ　7/00		7/00	Ｑ

審査請求　未請求　請求項の数36　ＯＬ　（全 22 頁）

(21)出願番号　特願平10－38840

(22)出願日　平成10年(1998)２月20日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　今村　紀代美
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　山川　輝二
神奈川県横浜市港北区新横浜２丁目４番19号　株式会社富士通プログラム技研内

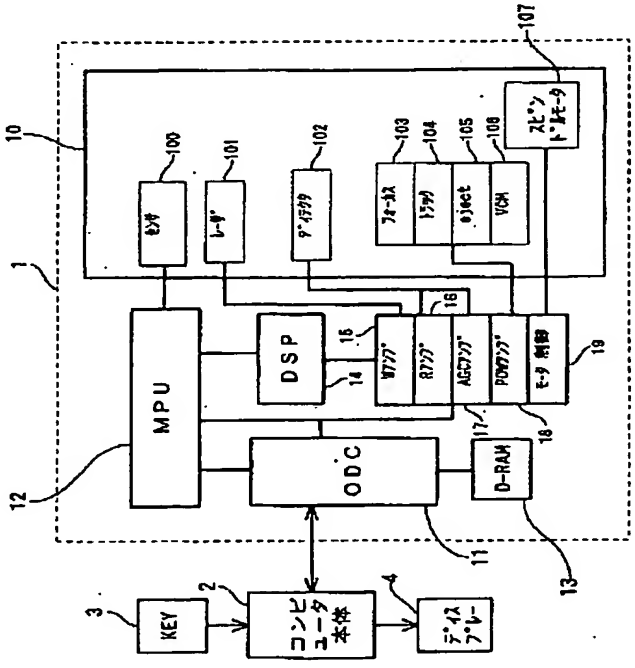
(74)代理人　弁理士　林　恒徳　（外１名）

(54)【発明の名称】　情報記憶装置及びその制御方法

(57)【要約】

【課題】記憶媒体に記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置を提供する。

【解決手段】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、第一の識別記号と第二の識別記号との対応関係に応じて、装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置が提供される。例えば、制御部は、第一の識別記号と第二の識別記号とが一致しない場合に、装着された記憶媒体に対する情報の読み出し及び書き込みを禁止し、第一の識別記号と第二の識別記号が一致した場合は、装着された記憶媒体に対する情報の読み出し及び書き込みを許可する。このように、情報記憶装置に記憶された識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可とすることで、情報の機密性が確保される。



【特許請求の範囲】
【請求項１】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、
記憶媒体の第一の識別記号を記憶する記憶部と、
装着された記憶媒体の第二の識別記号を獲得する識別記号獲得部と、
前記第一の識別記号と前記第二の識別記号との対応関係に応じて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置。
【請求項２】請求項１において、
前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果により、情報の読み出し及び／又は書き込みを禁止又は許可する判定を行うことを特徴とする情報記憶装置。
【請求項３】請求項１において、
前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、
前記制御部は、前記第一の識別記号と前記第二の識別記号との比較の結果と、前記読み出しアドレス情報に基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置。
【請求項４】請求項１又は３において、
前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、
前記制御部は、前記第一の識別記号と前記第二の識別記号との比較の結果と、該書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置。
【請求項５】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、
記憶媒体の第一の識別記号を記憶する記憶部と、
装着された記憶媒体の第二の識別記号を獲得する識別記号獲得部と、
前記装着された記憶媒体に対して第一のアドレス情報が指定されると、前記装着された記憶媒体から第二のアドレス情報を獲得するアドレス情報獲得部と、
前記第一の識別記号と前記第二の識別記号との対応関係と、前記第一のアドレス情報と前記第二のアドレス情報との対応関係に基づいて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする情報記憶装置。
【請求項６】請求項５において、
前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、
前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記読み出しアドレス情報に基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置。
【請求項７】請求項５又は６において、
前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、
前記制御部は、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置。
【請求項８】請求項１又は５において、
前記装着された記憶媒体はパスワードを有し、
前記制御部は、さらに、前記パスワードの判定により前記装着された記憶媒体の読み出し又は／及び書き込みのアクセス制御を行うことを特徴とする情報記憶装置。
【請求項９】請求項１又は５において、
前記制御部は、指示された設定コマンドに基づいて、前記第一の識別記号を前記記憶部に記録する制御を行うことを特徴とする情報記憶装置。
【請求項１０】請求項３又は６において、
前記制御部は、指示された前記読み出しアドレス情報を有する所定の設定コマンドに基づいて、前記読み出しアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。
【請求項１１】請求項４又は７において、
前記制御部は、指示された前記書き込みアドレス情報を有する所定の設定コマンドに基づいて、前記書き込みアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。
【請求項１２】請求項５において、
前記制御部は、指示された前記第二のアドレス情報を有する所定の設定コマンドに基づいて、前記第二のアドレス情報を前記装着された記憶媒体の所定領域に記録する制御を行うことを特徴とする情報記憶装置。
【請求項１３】請求項１０乃至１２のいずれかにおいて、
前記制御部は、前記装着された記憶媒体の前記所定領域に記録される情報を暗号化することを特徴とする情報記憶装置。
【請求項１４】請求項１３において、
前記制御部は、指示された暗号化情報を有する所定の設定コマンドに基づいて、前記装着された記憶媒体の前記所定領域に記録される情報を暗号化することを特徴とする情報記憶装置。
【請求項１５】請求項１０乃至１２において、
前記設定コマンドは、前記装着された記憶媒体の初期化コマンド又は設定のために設けられた特殊コマンドであることを特徴とする情報記憶装置。
【請求項１６】請求項１０乃至１２において、
前記制御部は、指示された解除コマンドに基づいて、前記所定領域を初期化することを特徴とする情報記憶装

置。
【請求項１７】請求項１０乃至１２において、
前記装着された記憶媒体の所定領域は、前記装着された記憶媒体のデータ領域以外に設定された媒体情報管理領域であることを特徴とする情報記憶装置。
【請求項１８】請求項１乃至１７のいずれかにおいて、
前記記憶媒体は、磁気ディスク、フロッピィディスク、光ディスク、光磁気ディスク、相変化型光ディスクのうちのいずれかの可換型記憶媒体であることを特徴とする情報記憶装置。
【請求項１９】請求項１乃至１８のいずれかにおいて、
前記第一及び第二の識別記号は、前記記憶媒体の製造番号であることを特徴とする情報記憶装置。
【請求項２０】記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置の制御方法において、
記憶媒体の第一の識別記号を記憶するステップ前記第一の識別記号を獲得するステップと、
装着された記憶媒体の第二の識別記号を獲得するステップと、
前記第一の識別記号と前記第二の識別記号との対応関係に応じて、前記装着された記憶媒体に対する情報の読み出し又は／及び書き込みのアクセス制御を行うステップとを有することを特徴とする情報記憶装置の制御方法。
【請求項２１】請求項２０において、
前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果により、情報の読み出し及び／又は書き込みを許可又は禁止する判定を行うことを特徴とする情報記憶装置の制御方法。
【請求項２２】請求項２０において、
前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、
前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号との比較の結果と、前記読み出しアドレス情報とに基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置の制御方法。
【請求項２３】請求項２０又は２２において、
前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、
前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号との比較の結果と、該書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置の制御方法。
【請求項２４】記憶媒体に対して第一のアドレス情報が指定されて情報の読み出し及び／又は書き込みを行う情報記憶装置の制御方法において、
第一の記憶媒体の第一の識別記号を記憶するステップ前記第一の識別記号を獲得するステップと、
装着された装着された記憶媒体の第二の識別記号を獲得するステップと、
前記第一のアドレス情報を獲得するステップと、
前記記憶媒体に設定された第二のアドレス情報を獲得するステップと、
前記第一の識別記号と前記第二の識別記号との対応関係と、前記第一のアドレス情報と前記第二のアドレス情報との対応関係とに基づいて、前記装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行うステップとを有することを特徴とする情報記憶装置の制御方法。
【請求項２５】請求項２４において、
前記装着された記憶媒体は、情報の読み出しを制御する読み出しアドレス情報を有し、
前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記読み出しアドレス情報とに基づいて、情報の読み出しを許可又は禁止することを特徴とする情報記憶装置の制御方法。
【請求項２６】請求項２４又は２５において、
前記装着された記憶媒体は、情報の書き込みを制御する書き込みアドレス情報を有し、
前記アクセス制御を行うステップは、前記第一の識別記号と前記第二の識別記号とを比較した結果と、前記第一のアドレス情報と前記第二のアドレス情報とを比較した結果と、前記書き込みアドレス情報とに基づいて、情報の書き込みを許可又は禁止することを特徴とする情報記憶装置の制御方法。
【請求項２７】請求項２０又は２４において、
前記装着された記憶媒体はパスワードを有し、
前記アクセス制御を行うステップは、さらに、前記パスワードの判定により前記装着された記憶媒体の読み出し及び／又は書き込みのアクセス制御を行うことを特徴とする情報記憶装置の制御方法。
【請求項２８】請求項２２又は２５において、
前記読み出しアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。
【請求項２９】請求項２３又は２６において、
前記書き込みアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。
【請求項３０】請求項２４において、
前記第二のアドレス情報を前記装着された記憶媒体の所定領域に記録するステップをさらに有することを特徴とする情報記憶装置の制御方法。
【請求項３１】請求項２７乃至３０のいずれかにおいて、
前記装着された記憶媒体の前記所定領域に記録される情報を暗号化するステップをさらに有することを特徴とする情報記憶装置の制御方法。
【請求項３２】請求項２７乃至３０において、

前記記録するステップは、前記装着された記憶媒体の初期化コマンド又は記録のために設けられた特殊コマンドに基づいて行われることを特徴とする情報記憶装置の制御方法。

【請求項３３】請求項２７乃至３０において、
前記所定領域の設定を解除する場合、前記所定領域を初期化することを特徴とする情報記憶装置の制御方法。

【請求項３４】請求項２７乃至３０において、
前記装着された記憶媒体の所定領域は、前記記憶媒体のデータ領域以外に設定された媒体情報管理領域であることを特徴とする情報記憶装置の制御方法。

【請求項３５】請求項２０乃至３４のいずれかにおいて、
前記記憶媒体は、磁気ディスク、フロッピィディスク、光ディスク、光磁気ディスク、相変化型光ディスクのうちのいずれかの可換型記憶媒体であることを特徴とする情報記憶装置の制御方法。

【請求項３６】請求項２０乃至３５のいずれかにおいて、
前記第一及び第二の識別記号は、前記記憶媒体の製造番号であることを特徴とする情報記憶装置の制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、光磁気ディスクなどの記憶媒体にデータ（情報）を記録する情報記憶装置に係り、特に、記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置に関する。

【０００２】

【従来の技術】一般に、光磁気ディスク（ＭＯ）などのようなデータの書き込みが可能な記憶媒体は、所定のデータ読み出し及び書き込みを行う情報記憶装置（以下、記憶装置という）に着脱可能となっており、装着された際、記憶装置によって、データの読み書きが行われる。また、記憶装置は、例えば、ＳＣＳＩケーブルなどで接続されたパーソナルコンピュータのような上位装置からのコマンドによって制御される。

【０００３】このような記憶媒体において、従来、互換性重視の観点から、データを書き込んだ記憶装置と異なる別の記憶装置によっても、そのデータの読み出し及び書き込みが可能である。

【０００４】図１８は、従来の記憶装置におけるデータの読み書きフローチャートである。ステップS1において、媒体が記憶装置に挿入されると、ステップS2において、媒体がロードされる。即ち、媒体は、記憶装置の所定位置に設置され、規定回転数で回転する。そして、ステップS3において、媒体の構成や記憶容量などの所定の媒体情報が読み出された後、この媒体情報に対応した動作や処理によってデータの読み出し及び書き込みが可能となる（ステップS4）。

【０００５】

【発明が解決しようとする課題】従って、記憶媒体さえ入手すれば、それに記録されている例えば顧客データベースや設計情報などの機密情報を容易に盗用又は改ざんすることができるという問題が生じていた。

【０００６】そこで、本発明の目的は、上記問題点に鑑み、記憶媒体に記録されたデータの機密性及びセキュリティを確保することができる情報記憶装置を提供することである。

【０００７】

【課題を解決するための手段】上記目的を達成するための本発明の情報記憶装置は、記憶媒体に対して情報の読み出し及び／又は書き込みを行う情報記憶装置において、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、第一の識別記号と第二の識別記号との対応関係に応じて、第二の記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする。

【０００８】例えば、制御部は、第一の識別記号と第二の識別記号とが一致しない場合に、装着された記憶媒体に対する情報の読み出し及び書き込みを禁止し、第一の識別記号と第二の識別記号が一致した場合は、装着された記憶媒体に対する情報の読み出し及び書き込みを許可する。

【０００９】このように、情報記憶装置に書き込まれた識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可とすることで、情報の機密性が確保される。

【００１０】また、装着された記憶媒体の所定領域は、情報の読み出しを制御する読み出しアドレス情報又は書き込みを制御する書き込みアドレス情報を有し、制御部は、第一の識別記号と第二の識別記号との比較の結果と、それぞれ読み出しアドレス情報又は書き込みアドレス情報とに基づいて、情報の読み出しを許可又は禁止するようにしてもよい。

【００１１】さらに、上記目的を達成するための本発明の情報記憶装置は、記憶媒体の第一の識別記号を記憶する記憶部と、装着された記憶媒体から第二の識別記号を獲得する識別記号獲得部と、装着された記憶媒体に対して第一のアドレス情報が指定されると、装着された記憶媒体から第二のアドレス情報を獲得するアドレス情報獲得部と、第一の識別記号と第二の識別記号との対応関係と、第一のアドレス情報と第二のアドレス情報との対応関係とに基づいて、装着された記憶媒体に対する情報の読み出し及び／又は書き込みのアクセス制御を行う制御部とを備えることを特徴とする。

【００１２】これにより、装着された記憶媒体に記録された複数の情報毎にセキュリティを設定することができる。

【００１３】また、装着された記憶媒体の所定領域は、

情報の読み出しを制御する読み出しアドレス情報又は書き込みアドレス情報を有し、制御部は、第一の識別記号と第二の識別記号が一致し、且つ第二のアドレス情報が第一のアドレス情報に含まれる場合、それぞれ読み出しアドレス情報又は書き込みアドレス情報に基づいて、情報の読み出しを許可又は禁止するようにしてもよい。

【００１４】さらに、上述のような構成の情報記憶装置において、制御部は、情報記憶装置と接続された情報記憶装置の制御装置から送られる所定の設定コマンドに基づいて、読み出しアドレス情報、書き込みアドレス情報又は第二のアドレス情報を、装着された記憶媒体の所定領域に記録する。そして、所定の設定コマンドは、例えば、スカジーインターフェースにおけるフォーマットコマンド又はベンダーユニークコマンドである。さらに、制御部は、上記制御装置から送られる所定の解除コマンドに基づいて、所定領域を初期化できることが好ましい。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について説明する。しかしながら、本発明の技術的範囲がこの実施の形態に限定されるものではない。なお、図において同一又は類似のものには同一の参照数字又は参照記号を付して説明する。

【００１６】本発明の実施の形態においては、データが記録される媒体として光磁気ディスク（ＭＯ）に基づいた説明を行うが、記憶媒体はこれに限定されるものではなく、例えば磁気ディスク、フロッピィディスク、光ディスク、相変化型光ディスクのような他の可換型記憶媒体であってもよい。

【００１７】図１は、本発明の実施の形態における光磁気ディスク装置の概略ブロック構成図である。図１によれば、光磁気ディスク装置１は、上位装置であるパーソナルコンピュータ２とＳＣＳＩインターフェースを介して接続されている。

【００１８】そして、光磁気ディスク装置１は、光磁気ディスクに対する書き込み及び読み出しを行う機構制御部１０を有し、さらに、本発明を実行するためのソフトウェアが格納されたファームウェアを有する光磁気ディスク制御部（ＯＤＣ）１１を備えた制御回路部を備える。

【００１９】制御回路部は、さらに、光磁気ディスク装置１の全体制御を行うＭＰＵ１２、読み取り／書き込み用バッファメモリであるＤ－ＲＡＭ１３、位置決め制御ををを行うＤＳＰ１４、書き込みデータ増幅回路１４、読み取りデータ増幅回路１６、ＡＧＣ増幅回路１７、ヘッド駆動用電力増幅回路１８及びディスク回転モータ制御回路１９を有する。

【００２０】機構制御部１０は、ヘッドセンサ１００、データ読み取り／書き込み用レーザダイオード１０１、ヘッドの傾きなどを検出するディテクタ１０２を有する。さらに、機構制御部１０は、ヘッド駆動用電力増幅回路１８により制御されるフォーカスアクチュエータ回路１０３、トラックアクチュエータ回路１０４，ディスク取り出し（イジェクト）モータ１０５及びヘッド駆動用ボイスコイルモータ１０６を有し、また、モータ制御回路１９により回転制御され、ディスクを回転するスピンドルモータ１０７を備える。

【００２１】一方、パーソナルコンピュータ２のキーボード３から入力されるオペレータの指示に対応し、コンピュータ２から光磁気ディスク制御部（ＯＤＣ）１１に対してＳＣＳＩコマンドが送信されて、データの書き込み／読み出し制御が行われる。また、コンピュータ２には、書き込みデータ及び読み出しデータを表示するディスプレー４が接続される。

【００２２】光磁気ディスク制御部（ＯＤＣ）１１は、フラッシュＲＯＭで構成されるファームウェアを有し、コンピュータ２から送られるＳＣＳＩコマンドを解析する機能を有する。さらに、ＳＣＳＩコマンドに対応して、ＭＰＵ１２と協働して、機構制御部１０に対して書き込み／読み出し制御を行う機能を有する。

【００２３】なお、本発明の適用は、ＳＣＳＩコマンド系に限定されず、ＡＴＡ／ＡＴＡＰＩ／ＳＡＳＩなどの他のコマンド体系でも適用できることはいうまでもない。

【００２４】図２は、光磁気ディスク（ＭＯ）のディスクフォーマットのレイアウト例であって、３．５インチ光磁気ディスクカートリッジに関するＩＳＯ規格により取り決められた媒体の領域区分である。図２に示されるように、円盤状のＭＯの中心から半径23.72mm から半径41.00mm の範囲が、使用者がデータ書き込み可能なデータ領域である。そして、その半径方向の内側と外側は、媒体の種類及び構成などの各種媒体情報が記録される媒体情報管理領域である。

【００２５】本発明の実施の形態においては、この媒体情報管理領域にセキュリティ領域が新たに設けられ、そのセキュリティ領域にあらかじめ記録されたセキュリティ情報である媒体の製造番号のような識別記号が、光磁気ディスク装置（以下、記憶装置という）に書き込まれる。または、例えば図２におけるインナーテストゾーン（Inner Test Zone)及びアウターテストゾーン（Outer Test Zone)のマニュファクチャラゾーン（for manufactures）やバッファゾーン(Buffer Zone）などをセキュリティ領域として代用してもよい。

【００２６】そして、あらかじめ識別記号であるセキュリティ情報が記録された光磁気ディスク（以下、媒体という）が、ある記憶装置に挿入されたとき、その記憶装置に書き込まれた識別記号と媒体にあらかじめ記録された識別記号との対応関係に応じて、データの読み書きを制御する。例えば、両識別記号が一致した場合のみ、データの読み書きを可能にする。即ち、媒体に書き込まれ

た識別記号と異なる識別記号を有する記憶装置では、その媒体におけるデータの読み書き不可とすることで、データの機密性が確保される。

【００２７】また、識別記号の記憶装置への書き込み処理は、上位装置からのセキュリティ設定コマンドに基づいて記憶装置の上記光磁気ディスク制御部（ＯＤＣ）１１において行われる。

【００２８】図３は、識別記号の記憶装置への書き込み処理フローチャートを示す図である。図３によれば、ステップS11 おいて、記憶装置がセキュリティ設定コマンドを受けると、ステップS12 において、記憶装置に既にセキュリティ情報が書き込まれているか否かが判断される。このとき、すでに書き込まれている場合、即ち既にセキュリティが設定されている場合は、ステップS13 において、書き込まれたセキュリティ情報の識別記号と、挿入されている記憶媒体の識別記号が比較される。そして、両識別記号が一致しない場合は、挿入された記憶媒体のセキュリティ確保のため、セキュリティ設定コマンドは異常終了する（ステップS19 ）。一方、セキュリティ情報が書き込まれていない初期状態である場合は、ステップS14 に進み、挿入されている記憶媒体の識別記号が読み出される。そして、ステップS15 において、その識別記号が記憶装置１のＯＤＣ１１の所定記憶領域に書き込まれる。また、後述するように、記憶媒体に記憶されているデータの一部にのみセキュリティが設定される場合は、ステップS16 において、セキュリティが設定されるデータのアドレス情報が記憶媒体のセキュリティ領域に書き込まれる。そして、ステップS17 において、記憶装置１は、セキュリティ設定コマンドで指定されたモードに変更され、セキュリティ設定コマンドは正常終了する（ステップS18 ）。

【００２９】図４は、パーソナルコンピュータ２から記憶装置１に送られるセキュリティ設定コマンドのＣＤＢ（コマンド・ディスクリプタ・ブロック）の例を示す図である。図４のセキュリティ設定コマンドは、ＳＣＳＩインターフェースにおけるベンダーユニーク(Vender Unique）コマンドを使用して設定される。そして、上述のように、媒体上に書き込まれた識別記号と挿入されている記憶装置の識別記号が一致したときのみ媒体にアクセス可能とするセキュリティ設定情報が、セキュリティ設定コマンドのセキュリティレベルに設定される。

【００３０】また、上記セキュリティレベルは、ベンダーユニークコマンドを利用したセキュリティ設定コマンドに代わって、通常のフォーマット(Format)コマンドに設定されてもよい。図５は、ＳＣＳＩコマンドにおいて、上記セキュリティレベルが設定されたフォーマットコマンドのＣＤＢの例を示す図である。

【００３１】図６は、上述のような記憶装置における本発明の第一の実施の形態であるセキュリティ処理のフローチャートである。以下に説明するセキュリティ処理は、記憶装置１の光磁気制御部（ＯＤＣ）１１において実行される。

【００３２】図６によれば、ステップS101において、媒体が記憶装置に挿入されると、ステップS102において、媒体がロードされる。即ち、媒体は、記憶装置の所定位置に設置され、規定回転数で回転する。そして、ステップS103において、媒体における上記媒体情報管理領域上の情報が読み出され、さらに、ステップS104において、その中の上記セキュリティ領域に書き込まれたセキュリティ情報（識別記号）が読み出される。

【００３３】ステップS105において、上記セキュリティ領域の情報が初期状態であるか否かが判断される。そして、上記セキュリティ領域が初期状態である場合、即ち、上記セキュリティ領域に識別記号が書き込まれていない場合、セキュリティが設定されていないものとして、ステップS108に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。

【００３４】一方、ステップS105において、セキュリティ領域に識別記号が書き込まれている場合、即ち、セキュリティが設定されている場合、ステップS106において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。

【００３５】そして、両者が一致する場合は、セキュリティが解除され、ステップS108に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。

【００３６】一方、ステップS106において、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS107）。

【００３７】このように、本発明の実施の形態においては、媒体上の媒体情報管理領域に、セキュリティ情報が書き込まれるセキュリティ領域が設けられる。そして、媒体が記憶装置にロードされた際、ロードされた記憶媒体の識別記号（セキュリティ情報）と、媒体に書き込まれた識別記号が一致しない場合は、データの読み書きを禁止することで、媒体が盗用された場合であっても、媒体に書き込まれたデータの機密性を確保することができる。

【００３８】ところで、上述の第一の実施の形態においては、媒体にセキュリティが設定された状態であっても、例えばその媒体を盗用した他人が媒体に書き込まれた識別記号と同じ識別記号を有する記憶装置を用いることによって、その媒体のデータの読み書きが可能である。

【００３９】そこで、媒体に書き込まれた識別記号と、その媒体がロードされた記憶装置の識別記号とが一致する場合であっても、データの読み書きを制限するセキュリティ機能が設定されることが好ましい。

【００４０】そのために、上記セキュリティ設定コマンド（図４）又はセキュリティレベルが設定されたフォーマットコマンド（図５）で指定されるパラメータのパラメータヘッダに読み出しアドレス情報と書き込みアドレス情報が設定される。図７は、上記各コマンドで指定されるパラメータの構成例である。パラメータは、図７（ａ）に示されるパラメータヘッドと、図７（ｂ）に示されるレベルディスクリプタから構成される。そして、上記各アドレス情報は、図７（ａ）のパラメータヘッドに設定される。なお、図７（ｂ）に示すレベルディスクリプタは、２バイト長のヘッダとそれに続くパラメタフィールドから構成される。そして、パラメタフィールドは、さらに機能属性ごとにページと呼ばれる単位に分類される。

【００４１】例えば、読み出しアドレス情報が設定されている場合は、識別記号が一致した場合であっても、データの読み出しが禁止される。また、読み出しアドレス情報が設定されていない場合は、データの読み出しは許可される。

【００４２】さらに、書き込みアドレス情報が設定されている場合は、識別記号が一致した場合であっても、データの書き込みが禁止される。また、書き込みアドレス情報が設定されていない場合は、データの書き込みは許可される。これら読み出しアドレス情報及び書き込みアドレス情報は、記憶装置の識別記号がセキュリティ領域に書き込まれる際に、同時にセキュリティ領域に書き込まれる。

【００４３】なお、読み出しアドレス情報又は書き込みアドレス情報が設定されていると、識別記号が一致した場合であっても、データの読み出し又は書き込みができなくなり不都合である。従って、読み出しアドレス情報又は書き込みアドレス情報が設定される場合は、同時に所定パスワードが設定され、各アドレス情報が設定されている場合であっても、パスワードが入力された場合は、読み出し又は書き込みが可能となるようにすることが好ましい。さらに、各アドレス情報の設定の有無に関わらず、所定パスワードが設定され、識別記号とパスワードの両方が一致した場合に、読み書きを許可することにより、セキュリティを二重に設定することが可能となり、よりデータの機密性を向上させることができる。

【００４４】また、パスワードは、上記パラメータのレベルディスクリプタに設定される。図８（ａ）は、レベルディスクリプタのパラメタフィールド（図７（ｂ）参照）におけるパスワードのページを示す図である。そして、このパスワードは、セキュリティ設定の際に、アドレス情報とともに、媒体のセキュリティ領域に書き込まれる。なお、図８（ｂ）は、レベルディスクリプタのパラメータフィールドにおける後述する論理ブロックアドレス（ＬＢＡ）の指定ページを示す図である。

【００４５】図９は、本発明の第二の実施の形態におけるセキュリティ処理のフローチャートである。本第二の実施の形態においては、上述のパラメータヘッダに読み出しアドレス情報が設定されていた場合である。図９においては、ステップS201乃至ステップS205は、上記図６におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【００４６】ステップS205において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS211に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS205において、セキュリティ情報が設定されている場合、ステップS206において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS207）。

【００４７】一方、両者が一致する場合は、ステップS208に進み、読み出しアドレス情報に基づいて、読み出し可否の判断が行われる。読み出しアドレス情報が設定されていない場合は、ステップS209に進み、データの読み出しが許可されるが、データの書き込みは禁止される。即ち、保存されているデータを読み込んで、その内容を見ることはできるが、そのデータの改変などの書き込みはできない。また、読み出しアドレス情報が設定されている場合は、ステップS210に進み、読み出し、書き込みともに禁止される。

【００４８】図１０は、本発明の第三の実施の形態におけるセキュリティ処理のフローチャートである。本第の実施の形態においては、上述のパラメータヘッダに上記書き込みアドレス情報が設定されていた場合である。図１０においては、ステップS301乃至ステップS305は、上記図６におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【００４９】ステップS305において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS311に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS305において、セキュリティが設定されている場合、ステップS306において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS307）。

【００５０】一方、両者が一致する場合は、ステップS308に進み、書き込みアドレス情報に基づいて、読み出し可否の判断が行われる。読み出しアドレス情報が設定されていない場合は、ステップS309に進み、データの書き込みが許可されるが、データの読み出し書き込みは禁止

される。即ち、新たなデータを作成することはできるが、保存されているデータを読み込むことはできない。また、読み出しアドレス情報が設定されている場合は、ステップS310に進み、読み出し及び書き込みともに禁止される。

【００５１】図１１は、本発明の第四の実施の形態におけるセキュリティ処理のフローチャートである。本第四の実施の形態においては、上述のパラメータヘッダに上記読み出しアドレス情報と書き込みアドレス情報がともに設定されていた場合である。

【００５２】ステップS405において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS415に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS405において、セキュリティ情報が設定されている場合、ステップS406において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、セキュリティが解除されず、データの読み書きが禁止される（ステップS407）。

【００５３】一方、両者が一致する場合は、ステップS408に進み、まず、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。そして、読み出しアドレス情報が設定されていない場合は、ステップS409に進み、次に書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップＳS410に示すように、データの読み出しと書き込みともに許可される。一方、ステップS409において、書き込みアドレス情報が設定されている場合は、ステップS411に示されるように、データの読み出しが許可されるが、データの書き込みは禁止される。

【００５４】また、ステップS408において、読み出しアドレス情報が設定されている場合は、ステップS412に進み、ステップS409同様に、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップＳS413に示すように、データの書き込みは許可されるが、データの読み出しは禁止される。一方、ステップS412において、書き込みアドレス情報が設定されている場合は、ステップS414に示されるように、データの読み出しと書き込みともに禁止される。

【００５５】上述の各実施の形態におけるデータの読み出しは、その媒体に保存されているデータ全てが対象である。しかしながら、媒体に複数のデータが保存されている場合に、その一部にのみセキュリティを設定したい場合が想定される。

【００５６】そのために、媒体にセキュリティ設定が行われるとき、上記図７のパラメータのレベルディスクリプタにセキュリティを設定したいデータの論理ブロックアドレス（ＬＢＡ）が指定される。さらに詳しくは、セキュリティを設定するデータを指定するためのＬＢＡ指定ページがレベルディスクリプタのパラメータフィールドに設定される（前述の図８（ｂ）参照）。そして、図８（ｂ）に示されるように、セキュリティを設定する１つデータのＬＢＡ（セキュリティＬＢＡ）が例えば３バイト長で指定される。このセキュリティＬＢＡの情報は、記憶装置の識別記号がセキュリティ領域に書き込まれる際に、同時にセキュリティ領域に書き込まれる。

【００５７】図１２は、本発明の第五の実施の形態におけるセキュリティ処理のフローチャートである。本第五の実施の形態は、上述の第二の実施の形態と同様に、読み出しアドレス情報が設定されている場合に、さらに、セキュリティＬＢＡが設定されている場合である。図１２においては、ステップS501乃至ステップS505は、上記図６におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【００５８】ステップS505において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS516に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS505において、セキュリティ情報が設定されている場合、ステップS506において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS507において、セキュリティ領域にセキュリティＬＢＡの指定の有無が判断される。そして、セキュリティＬＢＡの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS508）。

【００５９】一方、ステップS507において、セキュリティＬＢＡの指定がある場合は、ステップS509において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS510に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【００６０】また、含まれていないならば、ステップS511に進み、そのデータの読み出し及び書き込みが許可される。

【００６１】さらに、ステップS506において、両者の識別記号が一致する場合も、ステップS512において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS513に進み、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。

【００６２】そして、読み出しアドレス情報が設定されていない場合は、ステップS514に進み、データの読み出しが許可されるが、データの書き込みは禁止される。即ち、保存されているデータを読み込んで、その内容を見

ることはできるが、そのデータの改変などの書き込みはできない。また、読み出しアドレス情報が設定されている場合は、ステップS515に進み、読み出し、書き込みともに禁止される。

【００６３】また、ステップS512において、アクセスしているデータのＬＢＡがセキュリティＬＢＡが含まれていないならば、ステップS516に進み、データの読み出し及び書き込みともに許可される。

【００６４】図１３は、本発明の第六の実施の形態におけるセキュリティ処理のフローチャートである。本第六の実施の形態は、上述の第三の実施の形態と同様に、書き込みアドレス情報が設定されている場合に、さらに、セキュリティＬＢＡが設定されている場合である。図１３においては、ステップS601乃至ステップS605は、上記図６におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【００６５】ステップS605において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS616に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS605において、セキュリティ情報が設定されている場合、ステップS606において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS607において、セキュリティ領域にセキュリティＬＢＡの指定の有無が判断される。そして、セキュリティＬＢＡの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS608）。

【００６６】一方、ステップS607において、セキュリティＬＢＡの指定がある場合は、ステップS609において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS610に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【００６７】また、含まれていないならば、ステップS611に進み、そのデータの読み出し及び書き込みが許可される。

【００６８】さらに、ステップS606において、両者の識別記号が一致する場合も、ステップS612において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS613に進み、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。

【００６９】そして、書き込みアドレス情報が設定されていない場合は、ステップS614に進み、データの書き込みが許可されるが、データの読み出しは禁止される。即ち、新たなデータの作成は許可されるが、保存されているデータを見ることはできない。また、書き込みアドレス情報が設定されている場合は、ステップS615に進み、読み出し、書き込みともに禁止される。

【００７０】また、ステップS612において、アクセスしているデータのＬＢＡがセキュリティＬＢＡが含まれていないならば、ステップS616に進み、データの読み出し及び書き込みともに許可される。

【００７１】図１４は、本発明の第七の実施の形態におけるセキュリティ処理のフローチャートである。本第七の実施の形態は、上述の第三の実施の形態と同様に、読み出しアドレス情報及び書き込みアドレス情報が設定されている場合に、さらに、セキュリティＬＢＡが設定されている場合である。図１４においては、ステップS701乃至ステップS705は、上記図６におけるステップS101乃至ステップS105と同様であるので、その説明を省略する。

【００７２】ステップS705において、上記セキュリティ領域が初期状態である場合、セキュリティが設定されていないものとして、ステップS720に進み、媒体に書き込まれたデータの読み出し、及び媒体へのデータの書き込みが許可される。一方、ステップS705において、セキュリティ情報が設定されている場合、ステップS506において、読み出された識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。そして、両者が一致しない場合は、ステップS707において、セキュリティ領域にセキュリティＬＢＡの指定の有無が判断される。そして、セキュリティＬＢＡの指定がない場合は、媒体全体の読み出し及び書き込みが禁止される（ステップS708）。

【００７３】一方、ステップS707において、セキュリティＬＢＡの指定がある場合は、ステップS709において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS710に進み、そのデータの読み出し及びデータの書き込みが禁止される。

【００７４】また、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれていないならば、ステップS711に進み、そのデータの読み出し及び書き込みが許可される。

【００７５】さらに、ステップS706において、両者の識別記号が一致する場合も、ステップS512において、アクセスしているデータのＬＢＡが、セキュリティＬＢＡに含まれているか否かが判断される。含まれていれば、ステップS713に進み、まず、読み出しアドレス情報に基づいた読み出し可否の判断が行われる。そして、読み出しアドレス情報が設定されていない場合は、ステップS714に進み、次に書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップＳS715に示すように、データの読み出しと書き込みともに許可される。一方、ステップS715において、書き込みアドレス情報が設定されている場合は、ステップS716に示されるように、

データの読み出しが許可されるが、データの書き込みは禁止される。

【００７６】また、ステップS713において、読み出しアドレス情報が設定されている場合は、ステップS717に進み、ステップS714同様に、書き込みアドレス情報に基づいた書き込み可否の判断が行われる。そして、書き込みアドレス情報が設定されていない場合は、ステップS718に示すように、データの書き込みは許可されるが、データの読み出しは禁止される。一方、ステップS717において、書き込みアドレス情報が設定されている場合は、ステップS719に示されるように、データの読み出しと書き込みともに禁止される。また、ステップS712において、アクセスしているデータのＬＢＡがセキュリティＬＢＡが含まれていないならば、ステップS720に進み、データの読み出し及び書き込みともに許可される。

【００７７】そして、図１５は、上述した様々なセキュリティ処理が実行されるセキュリティ設定状態を解除するセキュリティ解除の処理フローチャートである。

【００７８】まず、ステップS801において、セキュリティ解除コマンドをコンピュータ２より記憶装置に送る。セキュリティ解除コマンドは、上記セキュリティ設定コマンドと同様に、ＳＣＳＩコマンドのベンダーユニークを利用して構成される。

【００７９】そして、ステップS802において、セキュリティ領域のアドレス情報が読み出され、ステップS803において、セキュリティ領域にセキュリティ情報の有無が確認される。セキュリティ情報が書き込まれている場合は、ステップＳ８０４に進み、セキュリティ情報に含まれる識別記号と、媒体が挿入されている記憶装置の識別記号とが比較される。一致する場合は、セキュリティ領域には、所定の初期値が書き込まれ、初期状態に戻される（初期化される）（ステップS805）。

【００８０】一方、識別記号が一致しない場合、若しくは元々セキュリティ領域にセキュリティ情報が書き込まれていない場合は、セキュリティ解除は行われない。

【００８１】なお、上記のフローチャートには図示されないが、セキュリティ情報がパスワードを有している場合は、パスワードを入力するステップが設けられ、セキュリティ情報に含まれるパスワードと、入力されたパスワードが一致した場合のみ、セキュリティ解除が実行されるようにしてもよい。

【００８２】上述した各本発明の実施の形態において、セキュリティ領域に書き込まれるセキュリティ情報（識別記号、アドレス情報、パスワードなど）は、さらに、機密性を高めるために暗号化されて書き込まれてもよい。この場合は、セキュリティ設定コマンドには、暗号化を指示する所定の暗号化情報が追加され、その暗号化情報に基づいて暗号化されたセキュリティ情報がセキュリティ領域に書き込まれる。

【００８３】図１６は、セキュリティ情報が暗号化されている場合における媒体ロード時の処理例のフローチャートである。図１６において、ステップS901において、記憶装置に媒体が挿入されると、ステップS902において、媒体ロードが開始される。そして、ステップS903において、媒体管理情報が読み出され、さらに、ステップS904において、その中におけるセキュリティ情報の有無が判断される。

【００８４】ステップS904において、セキュリティ情報がない場合は、ステップS909に進み、媒体におけるデータの読み出し及び書き込みが可能となる。

【００８５】一方、ステップS904において、セキュリティ情報がある場合は、次に、ステップS905において、セキュリティ情報が暗号化されているか否かが判断される。そして、ステップS906において、暗号化されている場合は、セキュリティ情報の暗号化が解除される。

【００８６】そして、ステップS907において、セキュリティ情報が有する識別記号と、現在媒体が挿入されている記憶装置の識別記号とが比較され、それらが一致しているか否かが判断される。両者が一致する場合は、セキュリティが解除され、ステップS909に進み、媒体におけるデータの読み出し及び書き込みが可能となる。

【００８７】一方、ステップS907において、両者が一致しない場合は、セキュリティが解除されず、媒体におけるデータの読み出し及び書き込みが不可能となる（ステップS908）。

【００８８】さらに、図１７は、図１６において、セキュリティ情報が、さらにパスワードを有する場合の媒体ロード時の処理例のフローチャートである。図１７によれば、図１６のフローチャートにステップS910が追加される。即ち、ステップS906において、暗号化が解除されると、入力されたパスワードとセキュリティ情報が有するパスワードとが比較される。そして、両者が一致しない場合は、セキュリティが解除されず、媒体におけるデータの読み出し及び書き込みが不可能となる（ステップS908）。

【００８９】一方、両者が一致する場合は、ステップS907に進み、さらに、上述した識別記号の比較が行われる。

【００９０】このとき、ステップS907とステップS910、即ち、パスワードの比較と識別記号の比較の順番は、反対であってもかまわない。そして、パスワードの比較のステップの設定、及び識別記号の比較のステップは、ユーザ又は記憶装置の製造業者若しくは販売業者によって任意に設定可能であって、その設定も任意に変更可能である。

【００９１】また、上記セキュリティ情報の暗号化は、例えば、ＤＥＳアルゴリズムや単純なビット並べ替えなどによって行われる。さらに、上記セキュリティ情報は、例えば、ASCII 、JIS 、EDICIBIC、ECU コードなどに変換されて上記セキュリティ領域に書き込まれてもよ

い。

【００９２】さらに、上述した各本発明の実施の形態においては、識別記号が一致した場合に読み出し又は書き込みを許可する制御が行われるが、不一致となった場合に許可するような制御が行われてもよい。

【００９３】

【発明の効果】以上説明したとおり、本発明によれば、光磁気ディスクのような記憶媒体の媒体情報管理領域に設けられたセキュリティ領域にあらかじめ記録された識別記号（セキュリティ情報）が、情報記憶装置固有の識別記号として書き込まれる。そして、このような記憶媒体が情報記憶装置に挿入された際、記憶媒体に記録された識別記号と、挿入された情報記憶装置の識別記号が一致しないときは、記憶媒体のデータにアクセス不可にすることで、データの機密性を確保することができる。このように、情報記憶装置に記憶された識別記号と異なる識別記号を有する記憶媒体は、その情報記憶装置での情報の読み書き不可とすることで、情報の機密性が確保される。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるデータ記憶装置のブロック構成図である。

【図２】光磁気ディスクのディスクフォーマットのレイアウト例である。

【図３】記憶装置への識別記号の書き込み処理フローチャートを示す図である。

【図４】ベンダーユニークコマンドを使用したセキュリティ設定コマンドのＣＤＢの構成例である。

【図５】セキュリティレベルが設定されたフォーマットコマンドのＣＤＢの構成例である。

【図６】本発明の第一の実施の形態におけるセキュリティ処理フローチャートである。

【図７】パラメータのパラメータヘッダ及びレベルディスクリプタの構成例である。

【図８】レベルディスクリプタのパラメタフィールドの構成例である。

【図９】本発明の第二の実施の形態におけるセキュリティ処理フローチャートである。

【図１０】本発明の第三の実施の形態におけるセキュリティ処理フローチャートである。

【図１１】本発明の第四の実施の形態におけるセキュリティ処理フローチャートである。

【図１２】本発明の第五の実施の形態におけるセキュリティ処理フローチャートである。

【図１３】本発明の第六の実施の形態におけるセキュリティ処理フローチャートである。

【図１４】本発明の第七の実施の形態におけるセキュリティ処理フローチャートである。

【図１５】セキュリティ解除の処理フローチャートである。

【図１６】セキュリティ情報が暗号化されている場合における媒体ロード時の処理例のフローチャートである。

【図１７】セキュリティ情報が暗号化され、さらに、パスワードが設定されている場合における媒体ロード時の処理例のフローチャートである。

【図１８】従来における媒体へのアクセス処理フローチャートである。

【符号の説明】

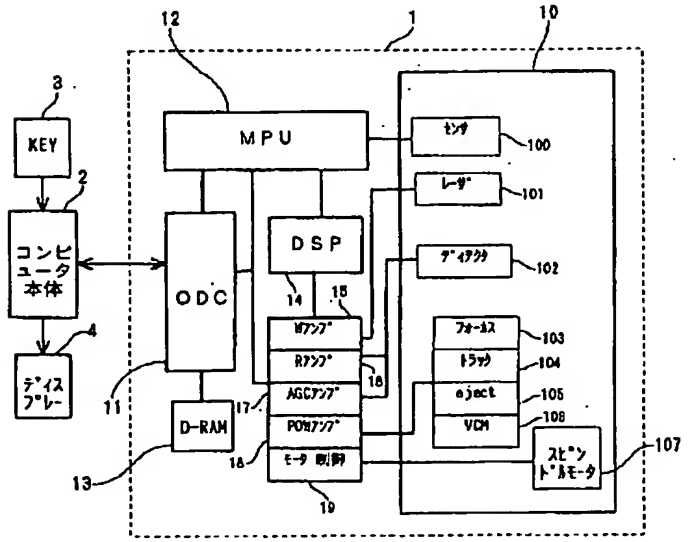
１　データ記憶装置

２　パーソナルコンピュータ

１０　機構制御部

１１　光磁気ディスク制御部

【図１】



【図２】

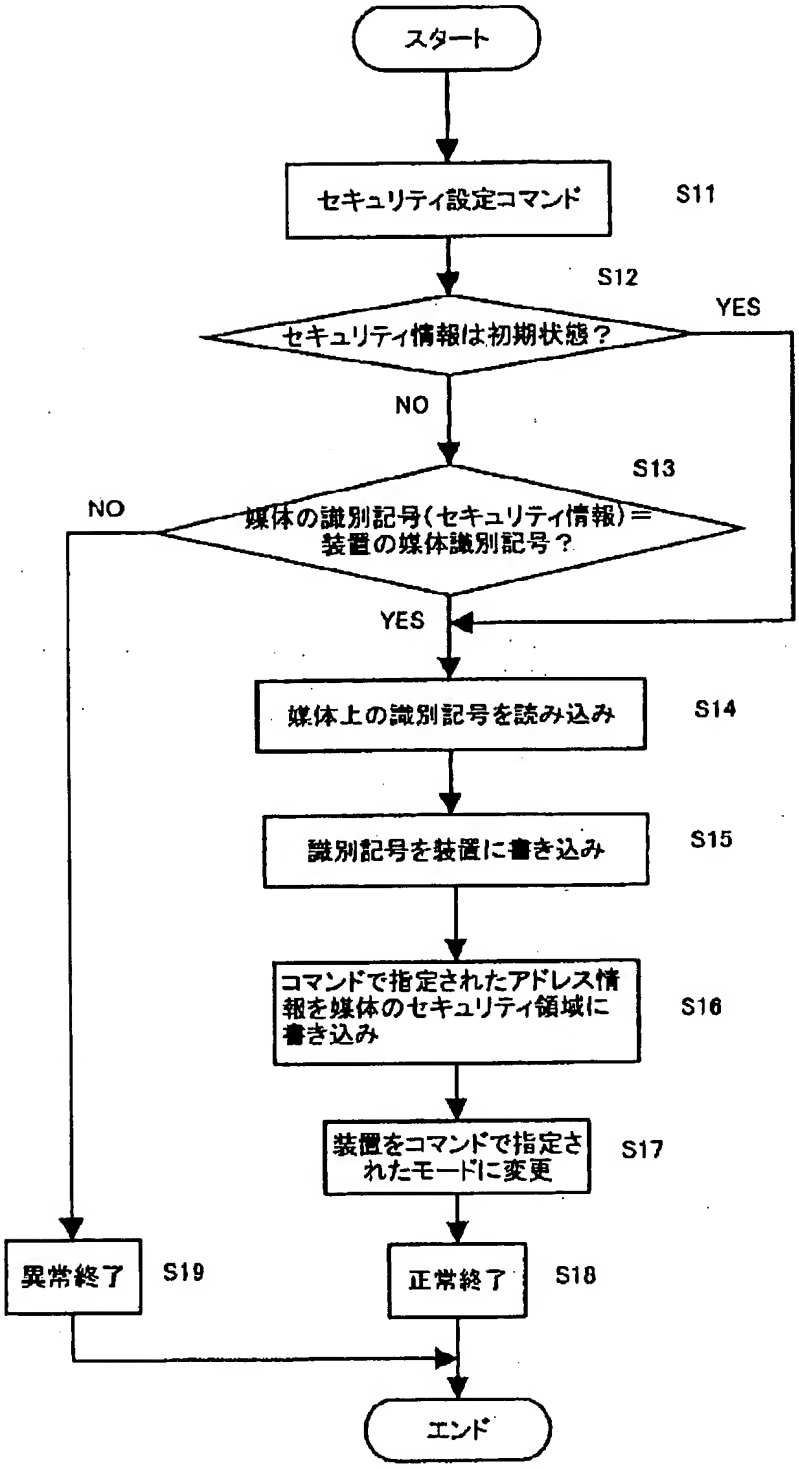
ゾーン名		半径mm	トラックNo.
Lead-in Zone			
	Initial Zone	22.60～23.14	
Acquire Zone			
	Lead-in tracks	23.14～23.60	-434～-93
	Focus tracks	23.60～23.61	-88～-85
Inner Test Zone			
	for manufacturers	23.61～23.65	-84～-53
	for drives	23.65～23.70	-52～-21
Inner Control Zone		23.70～23.72	-20～-5
Buffer Zone		23.72～23.72	-4～-1
Data Zone		23.72～41.00	0～18479
Outer Test Zone			
	for manufacturers	41.00～41.02	18480～18511
	for drives	41.02～41.06	18512～18543
Buffer Zone		41.06～41.28	18544～18854

媒体情報管理領域

データ領域

媒体情報管理領域

【図３】



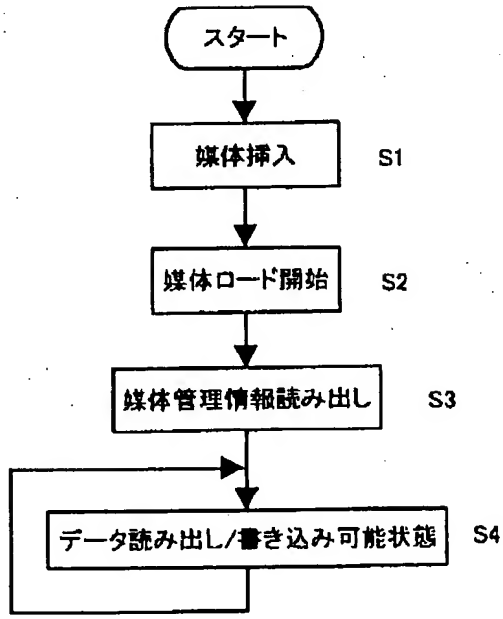
【図４】

		Bit							
		7	6	5	4	3	2	1	0
Byte	00	0	0	0	0	0	1	0	0
	01	LUN			FMT DATA	CMP LIST	DEFECT LIST FORMAT		
	02	セキュリティレベル							
	03	INTERLEAVE							
	04	INTERLEAVE							
	05	0	0	0	0	0	0	Flag	Link

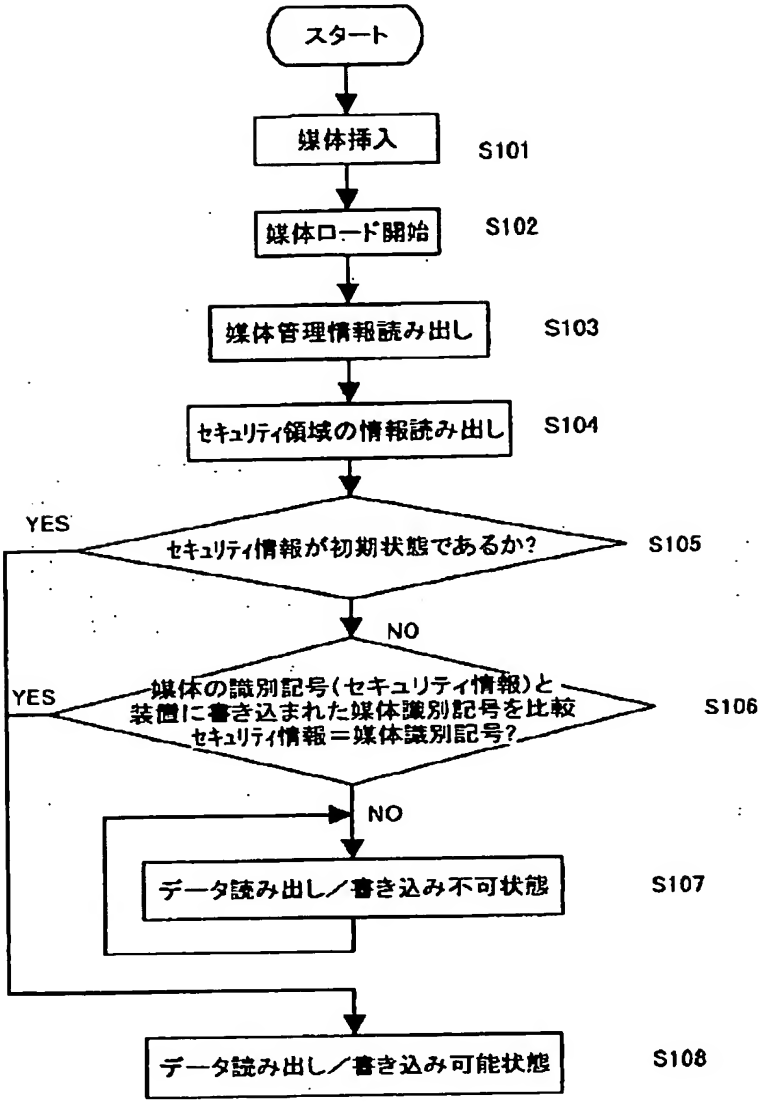
【図５】

		Bit							
		7	6	5	4	3	2	1	0
Byte	00	1	1	1	0	0	0	0	0
	01	LUN			0	0	0	0	0
	02	セキュリティレベル							
	03	X'00'							
	04	パラメタリスト長							
	05	0	0	0	0	0	0	Flag	Link

【図１８】



【図６】


スタート
媒体挿入
S101
媒体ロード開始
S102
媒体管理情報読み出し
S103
セキュリティ領域の情報読み出し
S104
YES
セキュリティ情報が初期状態であるか?
S105
NO
YES
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
セキュリティ情報＝媒体識別記号?
S106
NO
データ読み出し／書き込み不可状態
S107
データ読み出し／書き込み可能状態
S108

【図７】

(a)

Bit / Byte	7	6	5	4	3	2	1	0
0	X' 00'							
1	X' 00'							
2	X' 00'					書き込みアドレス情報	読み込みアドレス情報	LBASEIT
3	データブロック長							

(b)

Bit / Byte	7	6	5	4	3	2	1	0
0	セキュリティレベル							
1	ページコード							
:	パラメタフィールド							
n								

【図８】

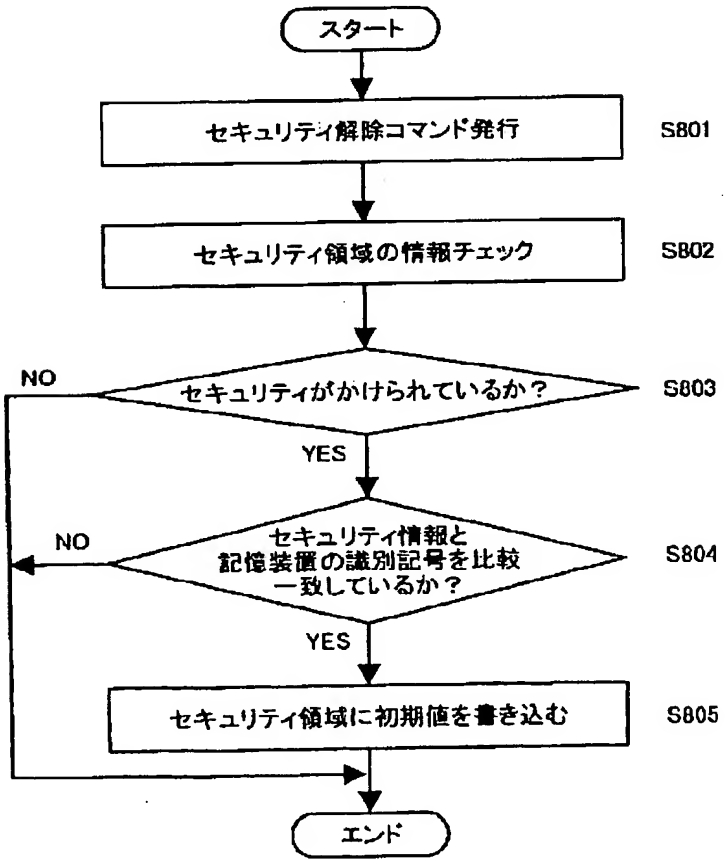
(a)

Bit / Byte	7	6	5	4	3	2	1	0
0	X' 01'							
1	X' 01'							
2～22	パスワード							

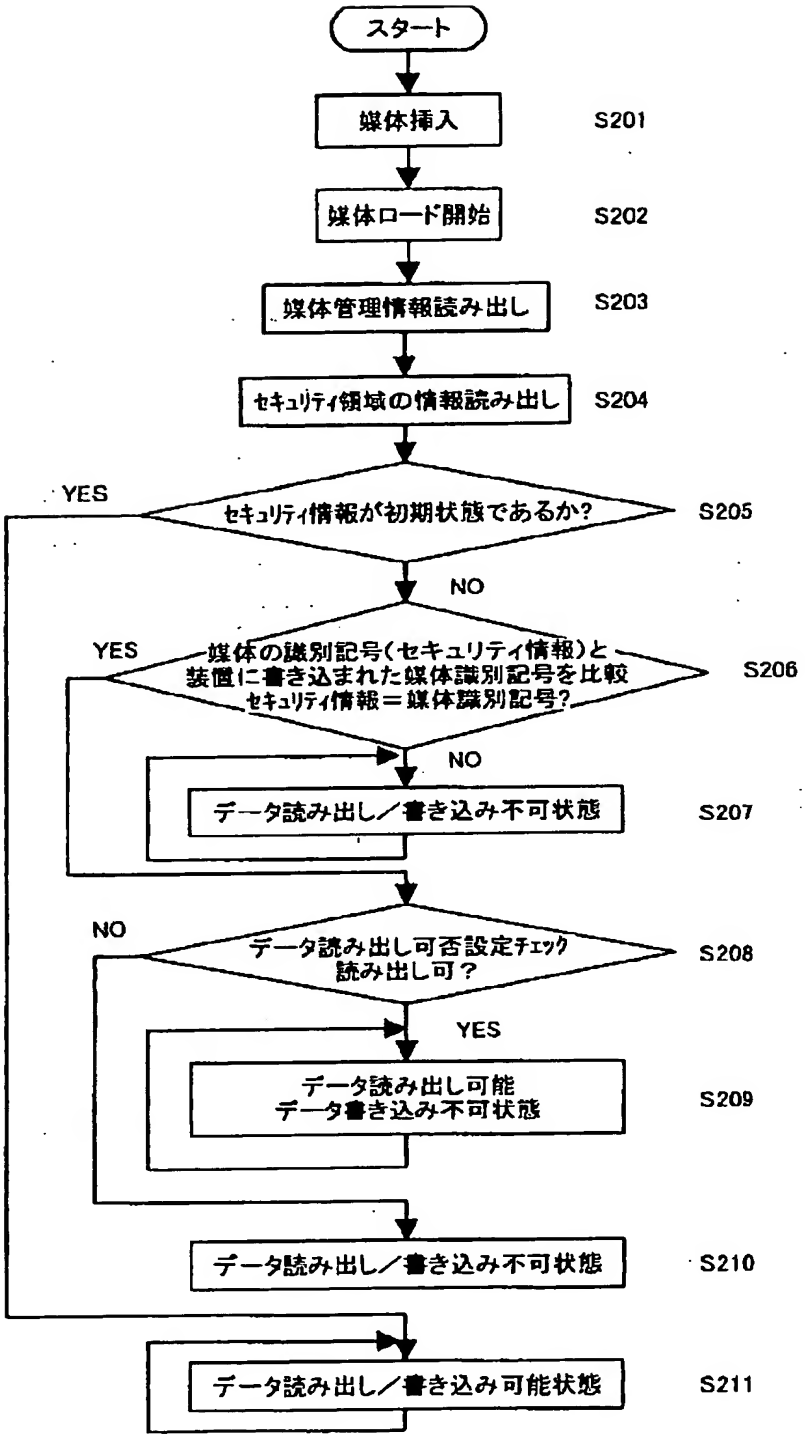
(b)

Bit / Byte	7	6	5	4	3	2	1	0
0	X' 01'							
1	X' 02'							
2	ページ長							
3～6	セキュリティ LBA							
:	セキュリティ LBA							
n～n+3	セキュリティ LBA							

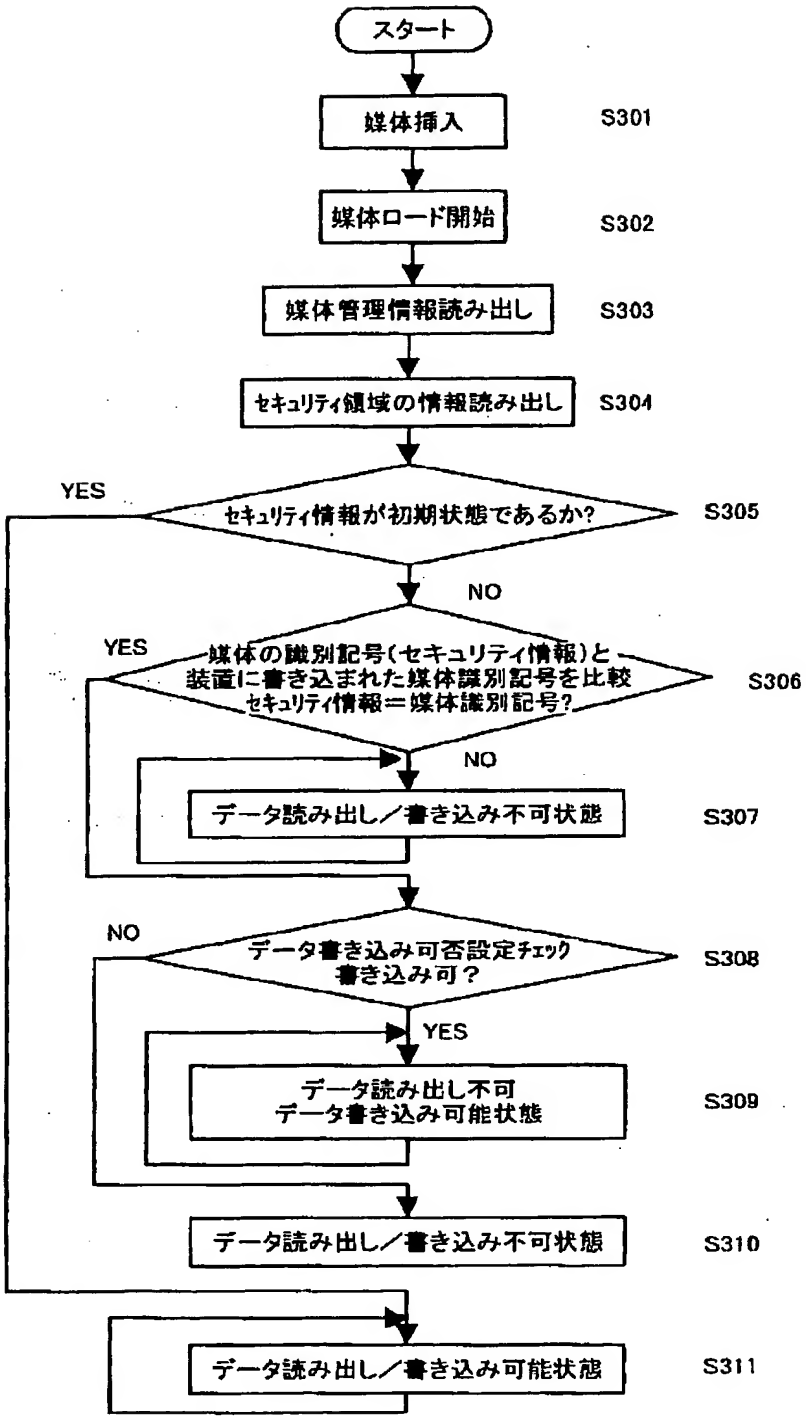
【図１５】



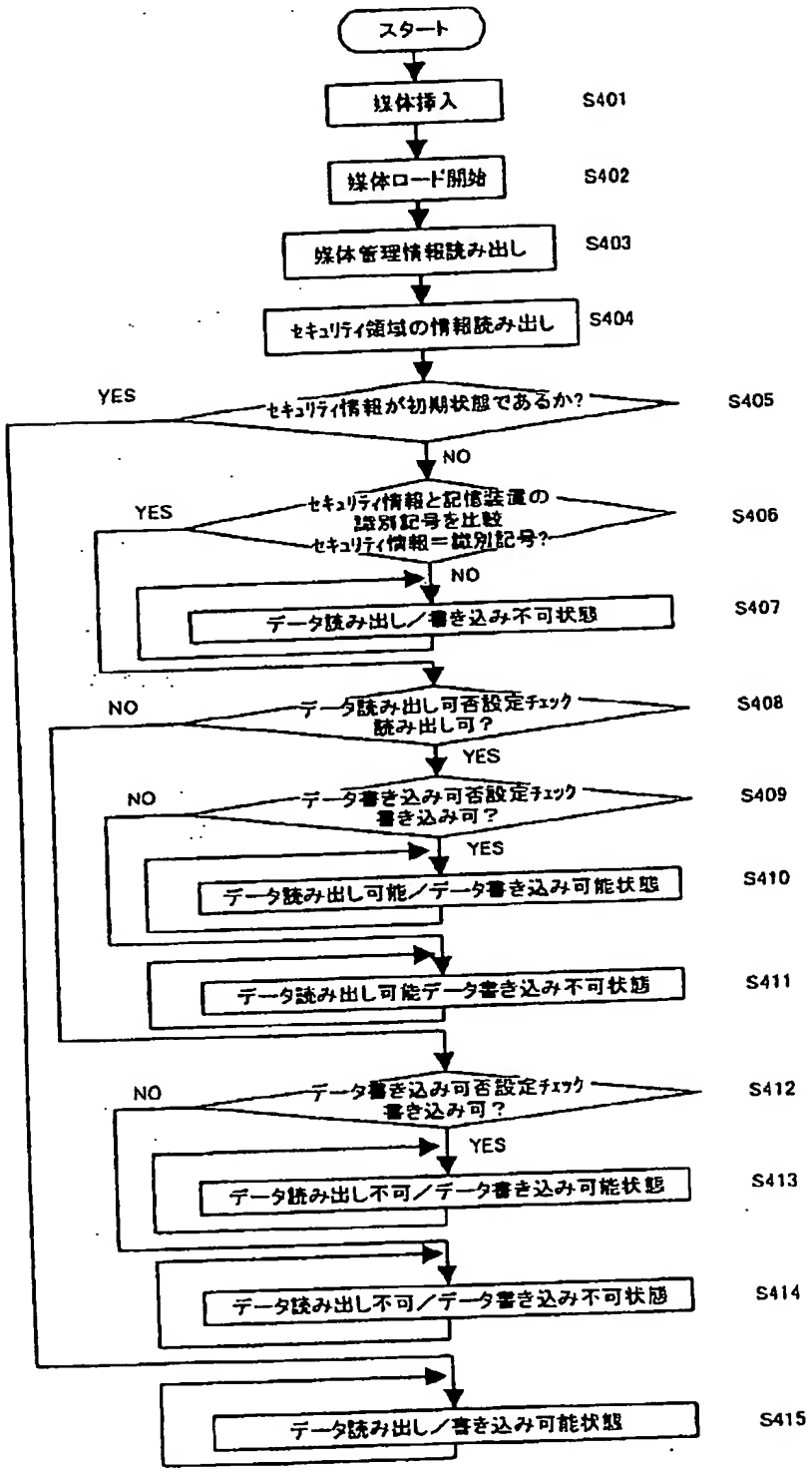
【図９】


スタート
媒体挿入
S201
媒体ロード開始
S202
媒体管理情報読み出し
S203
セキュリティ領域の情報読み出し
S204
YES
セキュリティ情報が初期状態であるか?
S205
NO
YES
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
セキュリティ情報＝媒体識別記号?
S206
NO
データ読み出し／書き込み不可状態
S207
NO
データ読み出し可否設定チェック
読み出し可？
S208
YES
データ読み出し可能
データ書き込み不可状態
S209
データ読み出し／書き込み不可状態
S210
データ読み出し／書き込み可能状態
S211

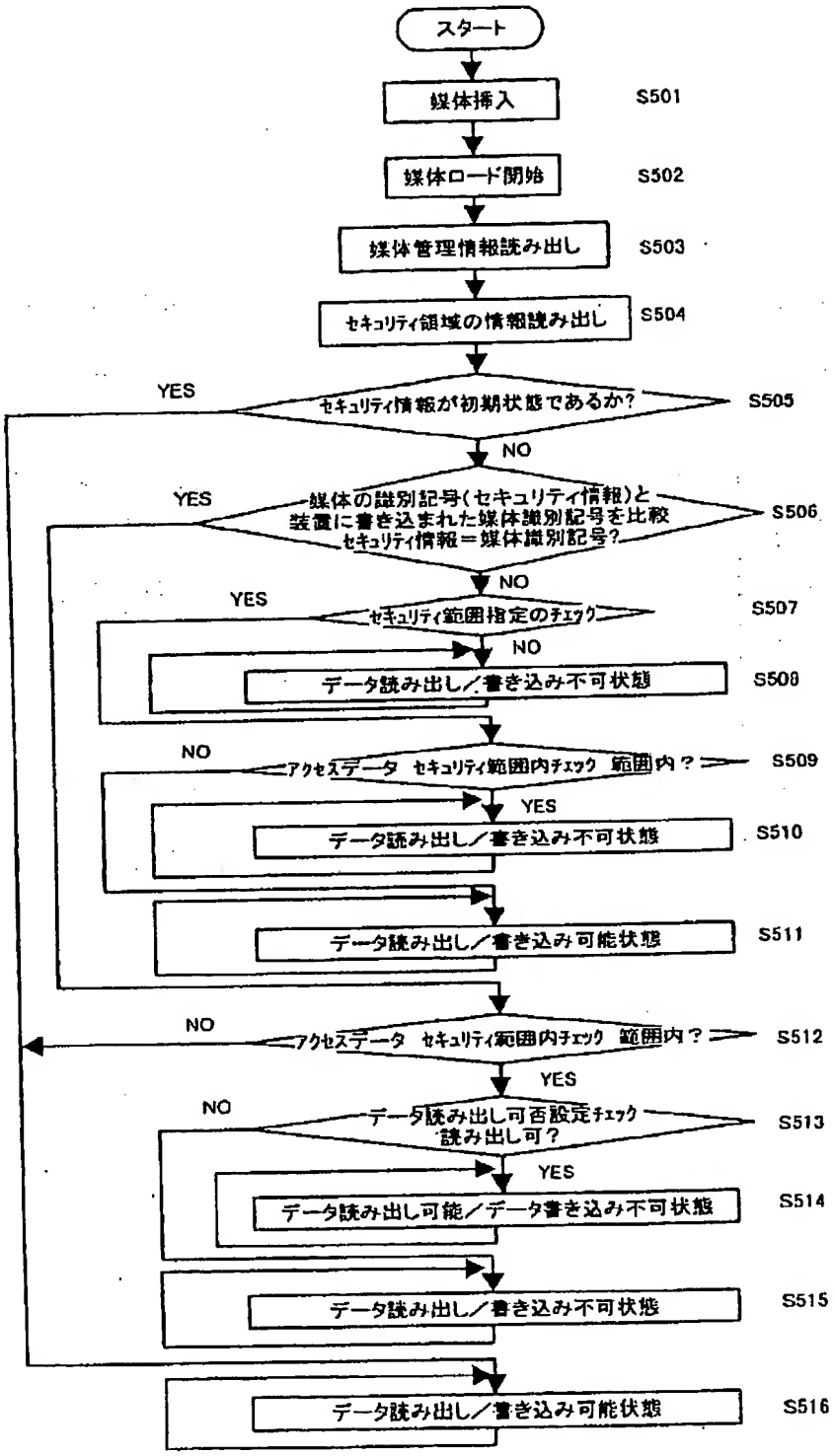
【図１０】


スタート
媒体挿入
S301
媒体ロード開始
S302
媒体管理情報読み出し
S303
セキュリティ領域の情報読み出し
S304
YES
セキュリティ情報が初期状態であるか?
S305
NO
YES
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
セキュリティ情報＝媒体識別記号?
S306
NO
データ読み出し／書き込み不可状態
S307
NO
データ書き込み可否設定チェック
書き込み可？
S308
YES
データ読み出し不可
データ書き込み可能状態
S309
データ読み出し／書き込み不可状態
S310
データ読み出し／書き込み可能状態
S311

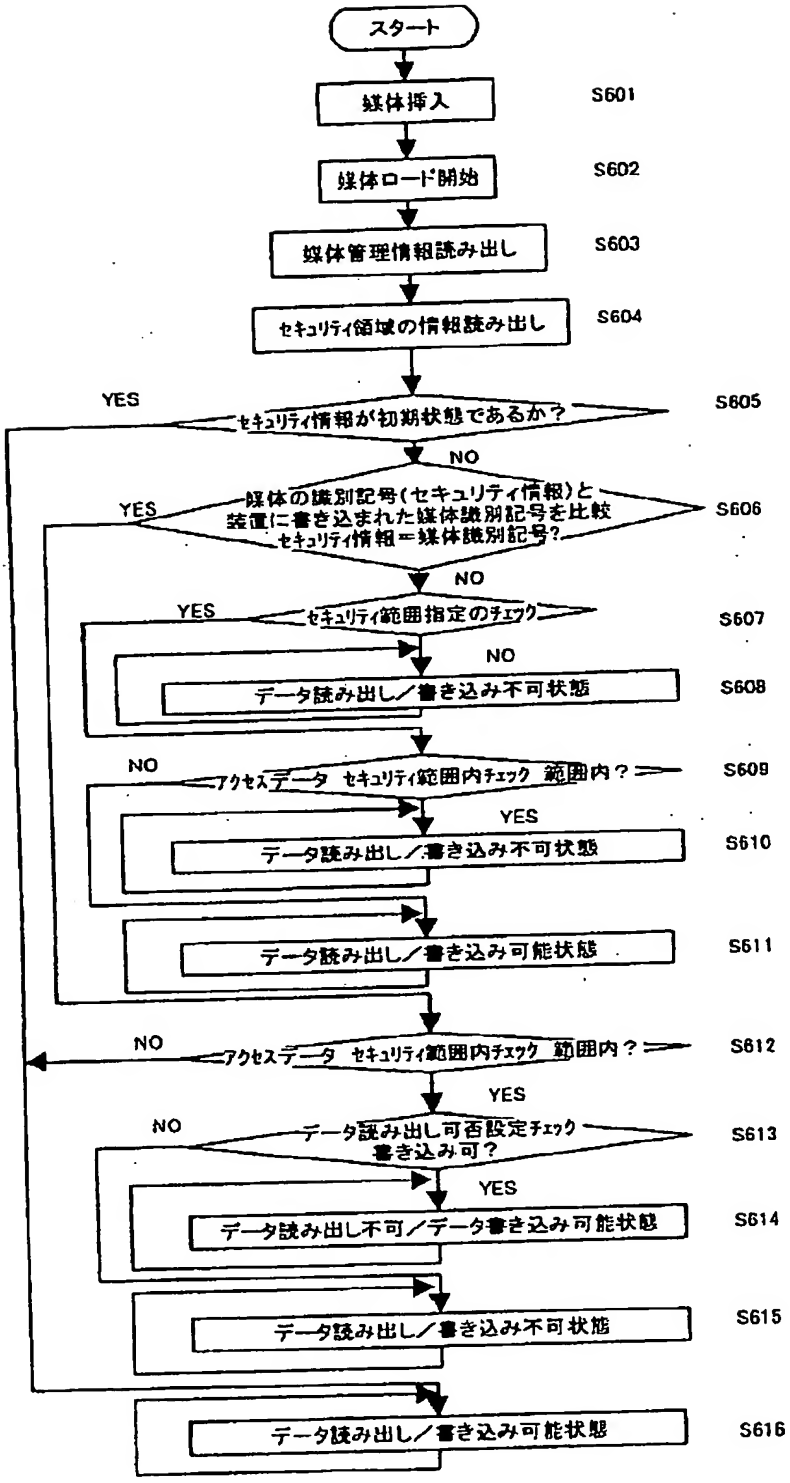
【図１１】


スタート
媒体挿入
S401
媒体ロード開始
S402
媒体管理情報読み出し
S403
セキュリティ領域の情報読み出し
S404
YES
セキュリティ情報が初期状態であるか?
S405
NO
YES
セキュリティ情報と記憶装置の識別記号を比較
セキュリティ情報＝識別記号?
S406
NO
データ読み出し／書き込み不可状態
S407
NO
データ読み出し可否設定チェック
読み出し可?
S408
YES
NO
データ書き込み可否設定チェック
書き込み可?
S409
YES
データ読み出し可能／データ書き込み可能状態
S410
データ読み出し可能データ書き込み不可状態
S411
NO
データ書き込み可否設定チェック
書き込み可?
S412
YES
データ読み出し不可／データ書き込み可能状態
S413
データ読み出し不可／データ書き込み不可状態
S414
データ読み出し／書き込み可能状態
S415

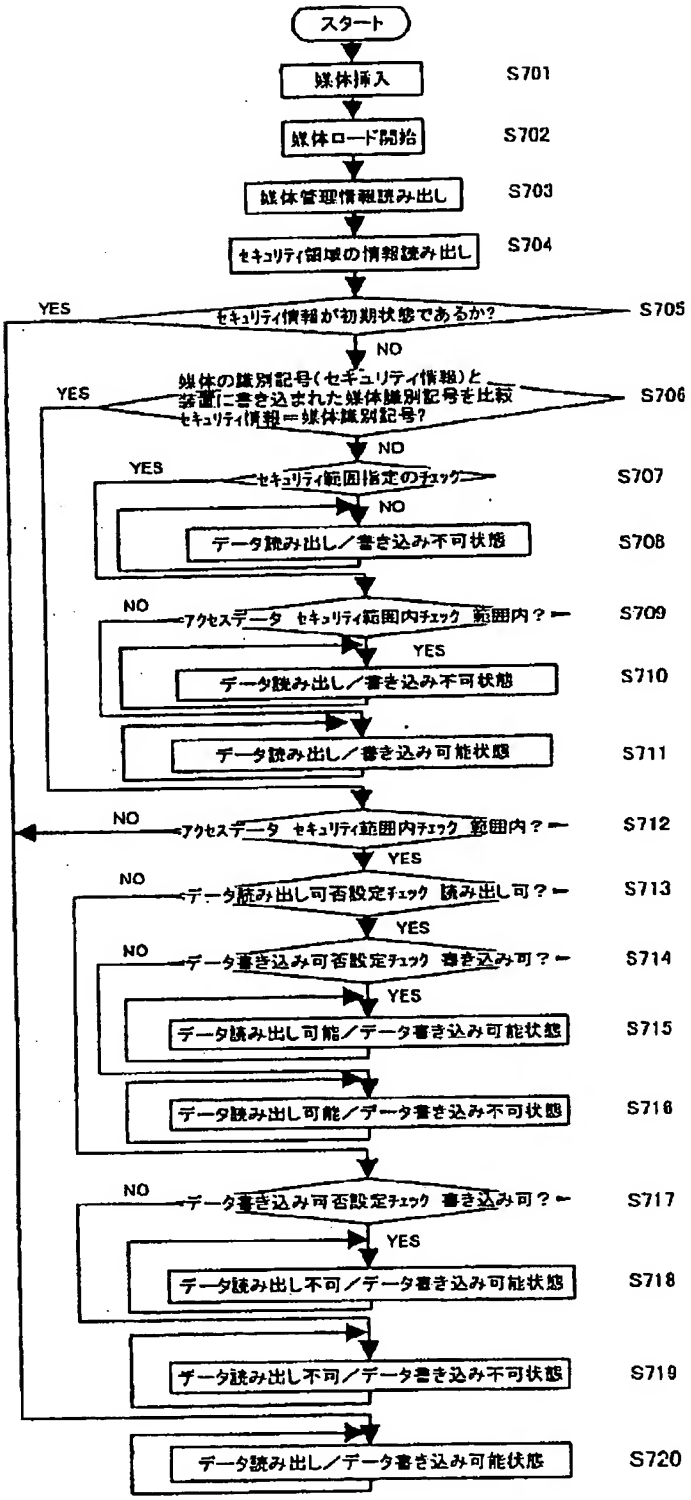
【図１２】


スタート
媒体挿入
S501
媒体ロード開始
S502
媒体管理情報読み出し
S503
セキュリティ領域の情報読み出し
S504
YES
セキュリティ情報が初期状態であるか?
S505
NO
YES
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
セキュリティ情報＝媒体識別記号?
S506
NO
YES
セキュリティ範囲指定のチェック
S507
NO
データ読み出し／書き込み不可状態
S508
NO
アクセスデータ　セキュリティ範囲内チェック　範囲内？
S509
YES
データ読み出し／書き込み不可状態
S510
データ読み出し／書き込み可能状態
S511
NO
アクセスデータ　セキュリティ範囲内チェック　範囲内？
S512
YES
NO
データ読み出し可否設定チェック
読み出し可？
S513
YES
データ読み出し可能／データ書き込み不可状態
S514
データ読み出し／書き込み不可状態
S515
データ読み出し／書き込み可能状態
S516

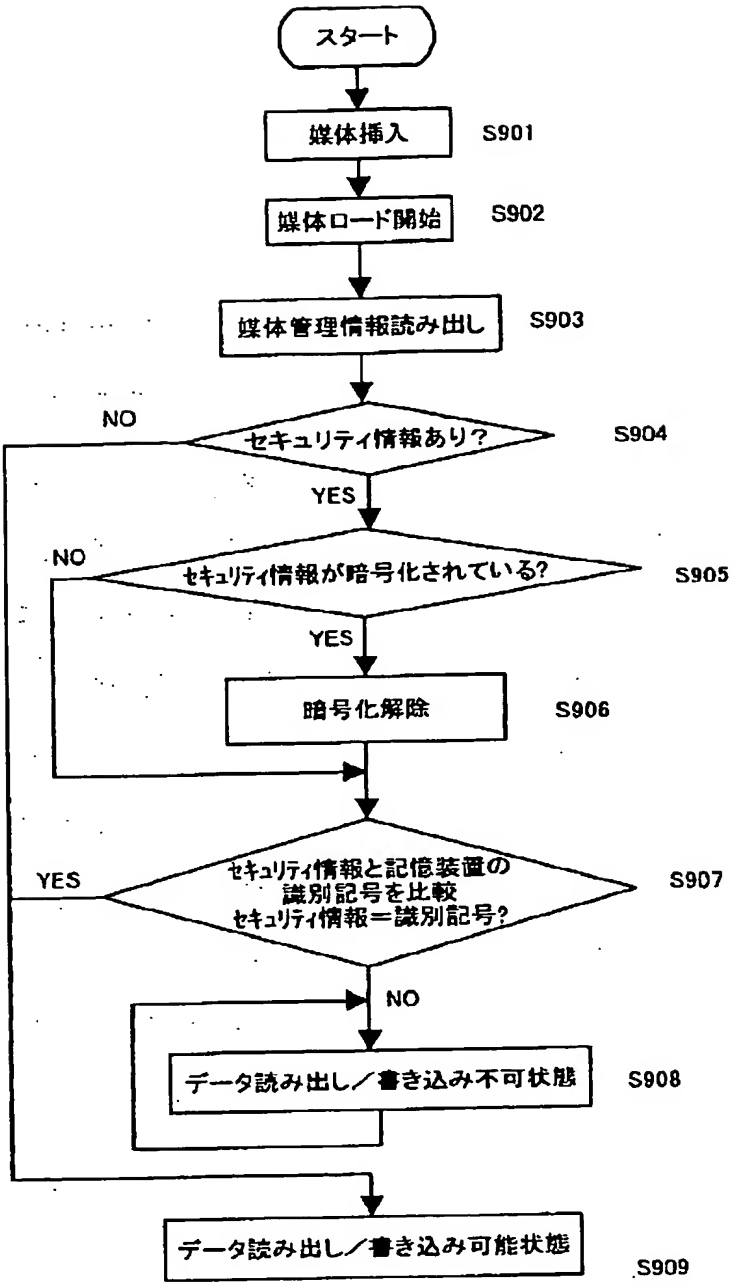
【図１３】


スタート
媒体挿入
S601
媒体ロード開始
S602
媒体管理情報読み出し
S603
セキュリティ領域の情報読み出し
S604
YES
セキュリティ情報が初期状態であるか？
S605
NO
YES
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
セキュリティ情報＝媒体識別記号?
S606
NO
YES
セキュリティ範囲指定のチェック
S607
NO
データ読み出し／書き込み不可状態
S608
NO
アクセスデータ セキュリティ範囲内チェック 範囲内？
S609
YES
データ読み出し／書き込み不可状態
S610
データ読み出し／書き込み可能状態
S611
NO
アクセスデータ セキュリティ範囲内チェック 範囲内？
S612
YES
NO
データ読み出し可否設定チェック
書き込み可？
S613
YES
データ読み出し不可／データ書き込み可能状態
S614
データ読み出し／書き込み不可状態
S615
データ読み出し／書き込み可能状態
S616

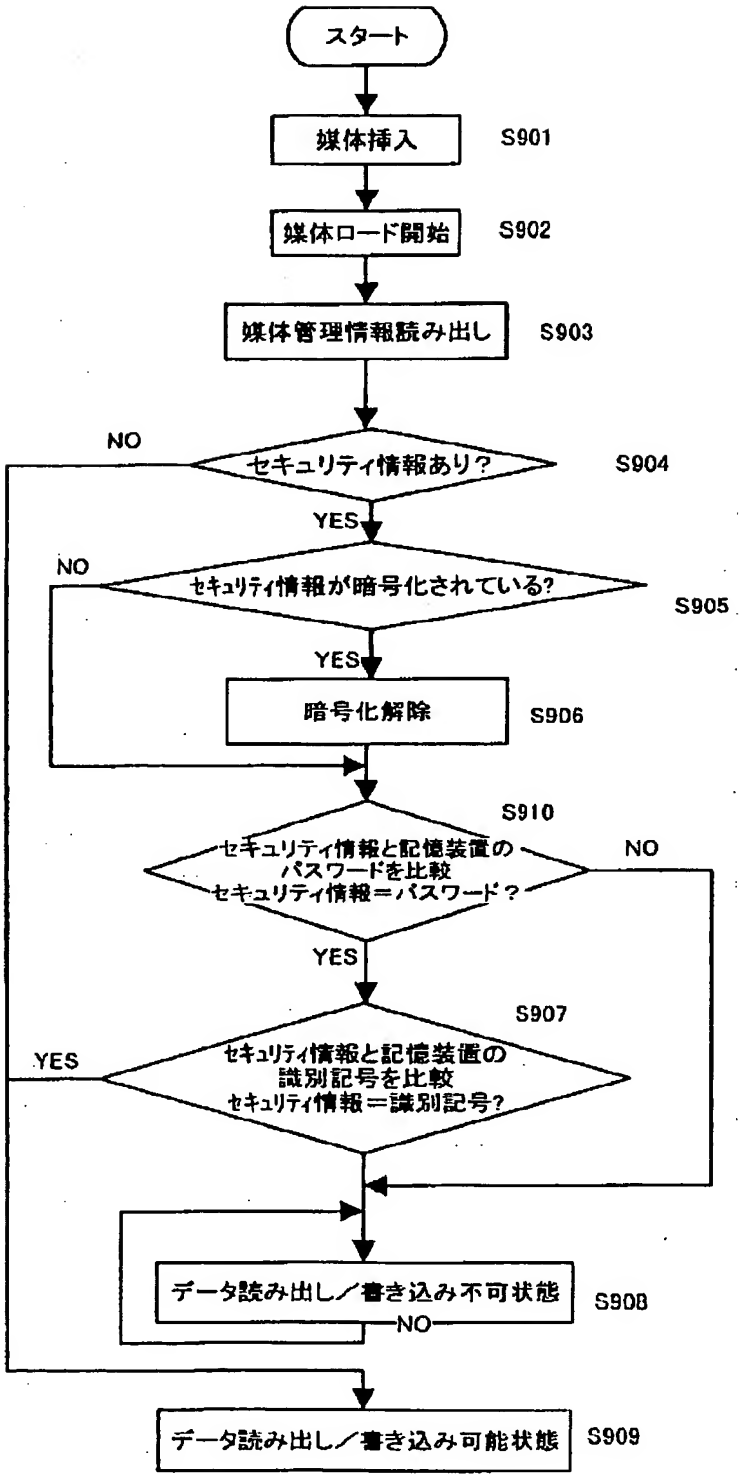
【図１４】


スタート
媒体挿入
S701
媒体ロード開始
S702
媒体管理情報読み出し
S703
セキュリティ領域の情報読み出し
S704
YES
セキュリティ情報が初期状態であるか?
S705
NO
媒体の識別記号(セキュリティ情報)と
装置に書き込まれた媒体識別記号を比較
YES
セキュリティ情報＝媒体識別記号?
S706
NO
YES
セキュリティ範囲指定のチェック
S707
NO
データ読み出し／書き込み不可状態
S708
NO
アクセスデータ　セキュリティ範囲内チェック　範囲内？
S709
YES
データ読み出し／書き込み不可状態
S710
データ読み出し／書き込み可能状態
S711
NO
アクセスデータ　セキュリティ範囲内チェック　範囲内？
S712
YES
NO
データ読み出し可否設定チェック　読み出し可？
S713
YES
NO
データ書き込み可否設定チェック　書き込み可？
S714
YES
データ読み出し可能／データ書き込み可能状態
S715
データ読み出し可能／データ書き込み不可状態
S716
NO
データ書き込み可否設定チェック　書き込み可？
S717
YES
データ読み出し不可／データ書き込み可能状態
S718
データ読み出し不可／データ書き込み不可状態
S719
データ読み出し／データ書き込み可能状態
S720

【図１６】


スタート
媒体挿入
S901
媒体ロード開始
S902
媒体管理情報読み出し
S903
NO
セキュリティ情報あり?
S904
YES
NO
セキュリティ情報が暗号化されている?
S905
YES
暗号化解除
S906
YES
セキュリティ情報と記憶装置の
識別記号を比較
セキュリティ情報＝識別記号?
S907
NO
データ読み出し／書き込み不可状態
S908
データ読み出し／書き込み可能状態
S909

【図１７】


スタート
媒体挿入
S901
媒体ロード開始
S902
媒体管理情報読み出し
S903
NO
セキュリティ情報あり？
S904
YES
NO
セキュリティ情報が暗号化されている?
S905
YES
暗号化解除
S906
S910
セキュリティ情報と記憶装置の
パスワードを比較
セキュリティ情報＝パスワード？
NO
YES
S907
YES
セキュリティ情報と記憶装置の
識別記号を比較
セキュリティ情報＝識別記号?
データ読み出し／書き込み不可状態
S908
NO
データ読み出し／書き込み可能状態
S909